CHRISTOPHER F. DRONEY, *Circuit Judge*, joined by DENNIS JACOBS, JOSÉ A. CABRANES, and REENA RAGGI, *Circuit Judges*, dissenting from the denial of rehearing *en banc*:

The majority opinion undertook the daunting task of attempting to apply a statute enacted decades ago to present technology. For example, who knew in 1986 that electronic mail—"email"—would become such a primary means of communication that its commercial providers would have millions of servers across the world to store and manage those communications? Or that the recipient of the warrant here—Microsoft—would itself manage over one million server computers, located in over forty countries, used by over one billion customers? Such developments in electronic communications could not have been anticipated at the time of the statute's adoption. Indeed, the task of applying statutes and rules from many years ago to unanticipated advances in technology has been undertaken in other contexts with much difficulty. *See, e.g.*, *United States v. Ganias*, 824 F.3d 199, 219–21 (2d Cir. 2016) (*en banc*). Thus, although I agree that reconsideration *en banc* should have occurred, I do so while recognizing the majority's efforts to solve the vexing issues presented here.

I dissent, though, from the denial of *en banc* in this case for three reasons. First, the privacy interests that are the focus of many aspects of the Stored Communications Act ("SCA") are protected in this context by its warrant requirement. Second, the activity that is the focus of the disclosure aspects of the SCA would necessarily occur in the United States where Microsoft is headquartered and where it would comply with the § 2703 warrant, not in the foreign country where it has chosen to store the electronic communications of its customers; also, the provisions of the statute concerning the mechanics of disclosure of these communications are unrelated to its privacy provisions. Third, the prudent course of action is to allow the warrants to proceed, and if Congress wishes to change the statute, it may do so while important criminal investigations continue.

When determining whether a statute applies extraterritorially, a court must read the statute provision by provision, not as a whole. *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090, 2103 (2016) (analyzing provisions individually to determine the focus of each). The court is then tasked with "determin[ing] whether the case involves a domestic application of the statute, and [does] this by looking to the statute's 'focus.'" *Id.* at 2101.

As the majority opinion notes, the SCA was broadly focused on the privacy concerns of electronic communications and the parties to those communications. *See* Maj. Op. at 33-36. But Congress addressed those concerns through the warrant requirement in the SCA. *See* 18 U.S.C. § 2703. That requirement provides protection for individual privacy interests by requiring the Government to make an adequate showing of probable cause of evidence of a crime or property used to commit a crime to a judge—a well-established standard of Fourth Amendment protection. *See id.*; Fed. R. Crim. P. 41(c); U.S. Const. amend. IV ("[N]o warrants shall issue, but upon probable cause."); *Camara v. Mun. Court of City & Cnty. of S.F.*, 387 U.S. 523, 528 (1967) (explaining that purpose of Fourth Amendment's probable cause requirement "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials").

Furthermore, the provisions of the SCA concerning the means of disclosure following obtaining the warrant are quite separate from the privacy components of the SCA. Section 2703 includes a number of specific disclosure provisions, which state it is the *provider* of the electronic communication service that is the source of the records sought by the Government either pursuant to the

warrant or the other means provided by that section to properly obtain the electronic communications. *See id.* § 2703 (a) ("A governmental entity may require the disclosure *by a provider* of electronic communication service of the contents of a wire or electronic communication . . . .") (emphasis added); § 2703 (b)(1) ("A governmental entity may require *a provider* of remote computing service to disclose the contents of any wire or electronic communication . . .") (emphasis added); § 2703 (c)(1) & (2) (both describing disclosure by providers); § 2703 (g) (same).

Thus, the only permissible reading of § 2703 is that it is the location of the provider of the electronic communication service that is relevant to determining whether the SCA is being applied extraterritorially under *RJR Nabisco*. Microsoft is headquartered in the United States, and there is no question that it would make the disclosure mandated by the § 2703 warrant in this country.

It makes no difference that Microsoft has chosen to store some electronic communications in other countries. That decision is based on its own business considerations, not privacy concerns for its customers. Microsoft has possession and immediate access to those emails regardless of where it chose to store them. Thus, the second prong of the *RJR Nabisco* test is satisfied here: the disclosure of

the electronic communications occurs in the United States, when Microsoft honors the warrant by disclosing those communications.

It is also important to note that the interests of foreign internet electronic communication service providers, whose headquarters are abroad and whose customers choose to subscribe to those services with the knowledge that the provider is located outside the United States, are not at stake here. If the emails sought by the Government in this case were maintained by a foreign-based internet service provider, the situation would be quite different. Here, however, the majority's concerns regarding "the interests of comity that . . . ordinarily govern the conduct of cross-boundary criminal investigations," Maj. Op. at 42, are overstated when the warrant is served on a U.S.-based electronic communication service provider for stored emails of a customer who *chose* to have a U.S.-based electronic communication service provider furnish his email service.

There is a real and practical component to the denial of *en banc* review of this case. This is a case that turns on statutory interpretation under *RJR Nabisco* rather than responding to a direct challenge to the constitutionality of the SCA or its disclosure provisions. The denial of *en banc* review hobbles both this specific

Government investigation as well as many others, important not only to the United States but also foreign nations. The Government's interest in continuing critical investigations into criminal activity is manifest. If Congress wishes to revisit the privacy and disclosure aspects of § 2703, it is free to do so when it chooses to do so. Until that time, this Court should allow the warrants to compel disclosure pursuant to § 2703 as it exists, and allow the Government to do its job in investigating serious criminal activity.

For these reasons, I respectfully dissent from the denial of *en banc* review.